Docket No. 242823US2RD

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Shinichi YASUDA, et al. GAU:

SERIAL NO: NEW APPLICATION EXAMINER:

FILED: HEREWITH

FOR: RANDOM NUMBER GENERATOR

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of **35 U.S.C. §120**.

☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of **35 U.S.C. §119(e)**: **Application No.** **Date Filed**

■ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of **35 U.S.C. §119**, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY	APPLICATION NUMBER	MONTH/DAY/YEAR
Japan	2002-269129	September 13, 2002

Certified copies of the corresponding Convention Application(s)

■ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

☐ were filed in prior application Serial No. filed

☐ were submitted to the International Bureau in PCT Application Number
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and

☐ (B) Application Serial No.(s)

- ☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Marvin J. Spivak
Registration No. 24,913
C. Irvin McClelland
Registration Number 21,124

Customer Number
22850
Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

JTSB-638

日　本　国　特　許　庁
JAPAN　PATENT　OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application:　２００２年　９月１３日

出願番号
Application Number:　特願２００２－２６９１２９

[ST.10/C]:　[ＪＰ２００２－２６９１２９]

出願人
Applicant(s):　株式会社東芝

２００３年　４月　４日

特許庁長官
Commissioner,
Japan Patent Office　太田信一郎

出証番号　出証特２００３－３０２３４６４

【書類名】　特許願

【整理番号】　13B026001

【提出日】　平成14年 9月13日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 7/58

【発明の名称】　乱数生成回路

【請求項の数】　8

【発明者】

【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

【氏名】　安田　心一

【発明者】

【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

【氏名】　藤田　忍

【特許出願人】

【識別番号】　000003078

【氏名又は名称】　株式会社　東芝

【代理人】

【識別番号】　100083806

【弁理士】

【氏名又は名称】　三好　秀和

【電話番号】　03-3504-3075

【選任した代理人】

【識別番号】　100068342

【弁理士】

【氏名又は名称】　三好　保男

【選任した代理人】

【識別番号】　100100712

【弁理士】

【氏名又は名称】　岩▲崎▼　幸邦

【選任した代理人】

【識別番号】　100100929

【弁理士】

【氏名又は名称】　川又　澄雄

【選任した代理人】

【識別番号】　100108707

【弁理士】

【氏名又は名称】　中村　友之

【選任した代理人】

【識別番号】　100095500

【弁理士】

【氏名又は名称】　伊藤　正和

【選任した代理人】

【識別番号】　100101247

【弁理士】

【氏名又は名称】　高橋　俊一

【選任した代理人】

【識別番号】　100098327

【弁理士】

【氏名又は名称】　高松　俊雄

【手数料の表示】

【予納台帳番号】　001982

【納付金額】　21,000円

【その他】　国等の委託研究の成果に係る特許出願（平成１４年度通信・放送機構「高度情報セキュリティに向けた真性乱数生成用集積回路の研究開発」委託研究、産業活力再生特別措置法第３０条の適用を受けるもの）

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　乱数生成回路

【特許請求の範囲】

【請求項１】　クロック信号をクロック入力端子に入力し、ランダム信号をカウントイネーブル端子に入力し、前記ランダム信号の変化に応じて前記クロック信号のカウント値を出力するカウンタ回路と、

前記ランダム信号の変化に応じて前記カウント値をラッチし第１の乱数信号を出力する第１のラッチ回路

とを備えることを特徴とする乱数生成回路。

【請求項２】　前記ランダム信号は、周波数の増加に対してパワースペクトルが減少する特性を有することを特徴とする請求項１に記載の乱数生成回路。

【請求項３】　周期が一定の乱数取得クロック信号と前記第１の乱数信号とを入力し、前記乱数取得クロック信号の変化に応じて前記第１の乱数信号をラッチし、第２の乱数信号を出力する第２のラッチ回路を更に備えることを特徴とする請求項１に記載の乱数生成回路。

【請求項４】　パルスカウンタを前記カウントイネーブル端子に接続し、前記パルスカウンタの出力を前記ランダム信号とすることを特徴とする請求項１に記載の乱数生成回路。

【請求項５】　ランダム信号を第１の入力端子に、クロック信号を第２の入力端子に入力し、前記ランダム信号と前記クロック信号の論理積を出力するアンド回路と、

前記論理積出力に応じてハイレベルとローレベルを交互に出力する分周ラッチ回路と、

前記ランダム信号の変化に応じて前記カウント値をラッチし乱数信号を出力する第１のラッチ回路

とを備えることを特徴とする乱数生成回路。

【請求項６】　前記ランダム信号は、周波数の増加に対してパワースペクトルが減少する特性を有することを特徴とする請求項５に記載の乱数生成回路。

【請求項７】　周期が一定の乱数取得クロック信号と前記第１の乱数信号と

を入力し、前記乱数取得クロック信号の変化に応じて前記第１の乱数信号をラッチし、第２の乱数信号を出力する第２のラッチ回路を更に備えることを特徴とする請求項５に記載の乱数生成回路。

【請求項８】　パルスカウンタを前記カウントイネーブル端子に接続し、前記パルスカウンタの出力を前記ランダム信号とすることを特徴とする請求項５に記載の乱数生成回路。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、乱数生成回路に係り、特に規則性のない乱数を生成する乱数生成回路に関する。

【０００２】

【従来の技術】

従来より、乱数による暗号化は、電子商取引や、無線通信等の情報通信において、パスワードの生成、暗号鍵生成、ＩＤ情報の生成、及びデジタル署名付加情報の生成等の情報の保護に用いられる。乱数の生成方法は、ソフトウェアによって発生させる方法が広く採用されている。しかし、ソフトウェアによる乱数生成方法は、プログラムに記載された数式に基づいて乱数を生成するため、何らかの規則性を有するという欠点がある。すなわち、規則性を有する暗号化は解読されてしまう可能性があり、個人情報の十分な保護が図れない問題があった。すなわち、周波数特性に依存しない乱数が求められていた。

【０００３】

これに対し、１／ｆ特性を有する雑音発生源から発生される雑音に基づいて、１／ｆ特性による周期性を持たない乱数を乱数生成回路により生成する方法がある（特許文献１参照。）。

【０００４】

特許文献１に記載の乱数生成回路は、図１６に示すように、雑音発生回路２０１，２０２と、雑音発生回路２０１，２０２の出力側にそれぞれ接続された差動回路２０３と、差動回路２０３の出力側に接続されたＡ／Ｄ変換回路２０４と、

Ａ／Ｄ変換回路２０４の出力側に接続された演算回路２０５とにより構成される。

【０００５】

先ず、雑音発生回路２０１，２０２は１／ｆ特性を有する雑音信号を出力する。次に、差動回路２０３は、雑音発生回路２０１，２０２から出力される２つの雑音信号の差動信号をアナログ信号として出力する。Ａ／Ｄ変換回路２０４は、差動回路から出力されるアナログ信号をデジタル信号に変換する。演算回路２０５は、デジタル変換された信号がスレシュホールドレベルに達しない場合には「０」を出力し、スレシュホールドレベルに達する場合には「１」を出力する。演算回路２０５は「０」と「１」の出現する確率が０．５になるようにスレシュホールドレベルを調節していた。

【０００６】

【特許文献１】

特開２００２－４１２８１号公報

【０００７】

【発明が解決しようとする課題】

しかし、図１６に示す乱数生成回路はフィルタ、差動回路等のアナログ回路と、２つの雑音発生回路を用いるため、専有面積が大きくなる問題があった。更に、「０」と「１」の出現する確率を演算回路２０５のスレッシュホールドレベルを変更し設定する必要があった。

【０００８】

本発明の目的は、複数の雑音発生回路を用いず、小型化が可能であり、周波数特性に依存しない乱数を生成し、「０」と「１」の出現する確率の調整を不要とすることが可能な乱数生成回路を提供することである。

【０００９】

【課題を解決するための手段】

上記目的を達成するために、本発明の第１の特徴は、クロック信号をクロック入力端子に入力し、ランダム信号をカウントイネーブル端子に入力し、ランダム信号の変化に応じてクロック信号のカウント値を出力するカウンタ回路と、ラン

ダム信号の変化に応じてカウント値をラッチし第１の乱数信号を出力する第１のラッチ回路とを備えることを要旨とする。

【００１０】

本発明の第１の特徴によれば、複数の雑音発生回路を用いず、小型化が可能であり、周波数特性に依存しない乱数を生成し、「０」と「１」の出現する確率の調整を不要とすることが可能な乱数生成回路を提供できる。

【００１１】

上記目的を達成するために、本発明の第２の特徴は、ランダム信号とクロック信号を入力し、ランダム信号及びクロック信号の論理積出力に応じてハイレベルとローレベルを交互に出力する分周回路と、ランダム信号の変化に応じてカウント値をラッチし乱数信号を出力するラッチ回路とを備えることを要旨とする。

【００１２】

本発明の第２の特徴によれば、複数の雑音発生回路を用いず、小型化が可能であり、周波数特性に依存しない乱数を生成し、「０」と「１」の出現する確率の調整を不要とすることが可能な乱数生成回路を提供できる。

【００１３】

【発明の実施の形態】

次に、図面を参照して本発明の第１～第５の実施の形態を説明する。以下の図面の記載において、同一または類似の部分には同一または類似の符号を付している。

【００１４】

先ず、第１～第５の実施の形態で用いられる「ランダム信号ＲＳ」について説明する。「ランダム信号ＲＳ」とは、オン幅とオフ幅の時間が一定でない複数の矩形波からなるデジタル信号である。また、「ランダム信号ＲＳ」は、周波数の増加に対してパワースペクトルが減少する特性を有する。矩形波の振幅は、一定であることが望ましいがここでは特に限定されない。例えば、ランダム信号ＲＳは、抵抗とコンデンサにより構成されるＣＲ遅延回路の遅延時間を利用した発振回路により生成される。抵抗やコンデンサの値がランダムに揺らぐこと利用して生成される。パワースペクトルが減少する信号の例としては、１／ｆ特性を有す

る揺らぎ信号等が挙げられる。「１／ｆ」とは、フーリエ分析したパワースペクトルがフーリエ周波数ｆに反比例して４５度の傾斜を持つものをいう。すなわち、配列、空間等の時系列データのスペクトル解析を行なうと、その両対数プロットで得られる傾きが－１を示す。

【００１５】

（第１の実施の形態）

本発明の第１の実施の形態に係る乱数生成回路１０ａは、図１に示すように、クロック信号ＣＳをクロック入力端子ＣＫに入力し、ランダム信号ＲＳをカウントイネーブル端子ＣＥに入力し、ランダム信号ＲＳの変化に応じてクロック信号ＣＳのカウント値を出力するカウンタ回路１と、ランダム信号ＲＳの変化に応じてカウント値をラッチし乱数信号ＲＮＳを出力する第１のラッチ回路３とを備える。更に、インバータ２が矩形波入力端子５１及びカウンタ回路１のカウントイネーブル端子ＣＥとの接続点と、第１のラッチ回路３のクロック入力端子ＣＫとの間に接続される。矩形波入力端子５１は、カウンタ回路１のカウントイネーブル端子ＣＥにランダム信号ＲＳを入力する端子である。クロック入力端子５２は、カウンタ回路１のクロック入力端子ＣＫに電気的に接続されたクロック信号ＣＳを入力する端子である。インバータ２の出力端子は、第１のラッチ回路３のクロック入力端子ＣＫに電気的に接続される。カウンタ回路１の出力端子Ｑは、第１のラッチ回路３の入力端子Ｄに電気的に接続される。第１のラッチ回路３の出力端子Ｑは、乱数出力端子５３に電気的に接続される。

【００１６】

本発明の第１の実施の形態に係る乱数生成回路１０ａの動作を、図２を用いて説明する。

【００１７】

（イ）先ず、時刻ｔ１において、図２（ａ）に示すように、矩形波入力端子５１に入力されるランダム信号ＲＳがローレベルからハイレベルとなる。

【００１８】

（ロ）時刻ｔ１からｔ２までの間、ランダム信号ＲＳがハイレベルの状態では、カウンタ回路１は、出力端子Ｑからカウント信号ＣＴＳを出力する。図２（ｃ

）に示すように、カウント信号ＣＴＳは、図２（ｂ）に示すクロック信号ＣＳの立ち上がりエッジ検出毎にハイレベルとローレベルを交互に切り換える。ここでは、カウンタ回路１は、例示的に１カウントごとにローレベルとハイレベルが交互に切り換わる１ビットカウンタであるとする。

【００１９】

（ハ）時刻ｔ２において、ランダム信号ＲＳがハイレベルからローレベルとなる。ランダム信号ＲＳがローレベルとなると、インバータ２は、図２（ｄ）に示すように、ハイレベルとなるランダム反転信号ＲＳバーを出力する。ランダム反転信号ＲＳバーがハイレベルとなると、第１のラッチ回路３は、クロック入力端子ＣＫの立ち上がりエッジでカウンタ回路１から出力されるカウント信号ＣＴＳをラッチし、図２（ｅ）に示すように、乱数信号ＲＮＳを出力する。

【００２０】

（ニ）時刻ｔ３において、再びランダム信号ＲＳがローレベルからハイレベルとなる。カウンタ回路１は、ランダム信号ＲＳがハイレベルの状態が続く間、クロック信号ＣＳの立ち上がりエッジ検出毎に、カウント信号ＣＴＳのレベルを交互に切り替える。

【００２１】

（ホ）時刻ｔ４において、ランダム信号ＲＳがハイレベルからローレベルとなる。ランダム信号ＲＳがローレベルとなると、インバータ２は、図２（ｄ）に示すように、ハイレベルとなるランダム反転信号ＲＳバーを出力する。ランダム反転信号ＲＳバーがハイレベルとなると、第１のラッチ回路３は、クロック入力端子ＣＫの立ち上がりエッジでカウンタ回路１から出力されるカウント信号ＣＴＳをラッチし、図２（ｅ）に示すように、乱数信号ＲＮＳを出力する。以後、同様にランダム信号ＲＳの立ち下がりエッジで乱数信号ＲＮＳを出力する動作を繰り返す。

【００２２】

次に、乱数信号ＲＮＳの出力が「０」または「１」である確率を図３を用いて説明する。ただし、ランダム信号ＲＳはｙ＝Ｆ（ｓ）の関数であると仮定して模式的に説明する。ランダム信号ＲＳを構成するランダムな矩形波のオン幅をＴ、

最小オン幅をＴｍｉｎ、最大オン幅をＴｍａｘとする。また、最大オン幅Ｔｍａｘから最小オン幅Ｔｍｉｎを引いたオン幅領域ＴＺから分解能設定クロック信号ＳＣの周期で割った値を分割数Ｎとする。オン幅領域ＴＺは、ランダムな矩形波の発生源となる抵抗、ダイオード等の素子が持つ周波数特性、矩形波を出力する回路の特性、及びフィルタ等の特性等によって決められる。この時、オン幅Ｔのランダムな矩形波の分布関数をＦ（ｔ）とすると、分割数Ｎが偶数の時に乱数生成回路から「０」が出力される確率Ｐｔ（０）は、

【数１】

$$Pt(0)=\int_{T\,min}^{T\,min+\frac{\Delta T}{N}}F(t)dt+\int_{Tmin+\frac{2\Delta T}{N}}^{T\,min+\frac{3\Delta T}{N}}F(t)dt+\cdots+\int_{Tmin+\frac{(N-2)\Delta T}{N}}^{T\,min+\frac{(N-1)\Delta T}{N}}F(t)dt \quad \cdots(1)$$

で表される。

【００２３】

分割数Ｎが偶数の時に乱数生成回路から１が出力される確率Ｐｔ（１）は、

【数２】

$$Pt(1)=\int_{T\,min+\frac{\Delta T}{N}}^{T\,min+\frac{2\Delta T}{N}}F(t)dt+\int_{Tmin+\frac{3\Delta T}{N}}^{T\,min+\frac{4\Delta T}{N}}F(t)dt+\cdots+\int_{Tmin+\frac{(N-1)\Delta T}{N}}^{Tmax}F(t)dt \quad \cdots(2)$$

で表される。

【００２４】

また、分割数Ｎが奇数の時に乱数生成回路から０が出力される確率Ｐｔ（０）は、

【数３】

$$Pt(0)=\int_{T\,min}^{T\,min+\frac{\Delta T}{N}}F(t)dt+\int_{Tmin+\frac{2\Delta T}{N}}^{T\,min+\frac{3\Delta T}{N}}F(t)dt+\cdots+\int_{Tmin+\frac{(N-1)\Delta T}{N}}^{Tmax}F(t)dt \quad \cdots(3)$$

で表される。

【００２５】

分割数Ｎが奇数の時に乱数生成回路から１が出力される確率Ｐｔ（１）は、

【数４】

$$Pt(1)=\int_{T\min+\frac{\Delta T}{N}}^{T\min+\frac{2\Delta T}{N}}F(t)dt+\int_{T\min+\frac{3\Delta T}{N}}^{T\min+\frac{4\Delta T}{N}}F(t)dt+\cdots+\int_{T\min+\frac{(N-2)\Delta T}{N}}^{T\min+\frac{(N-1)\Delta T}{N}}F(t)dt \quad \cdots(4)$$

で表される。

【００２６】

ここで、分割数Ｎが偶数となる場合の０と１が出る頻度の差はＰｔ（０）－Ｐｔ（１）で表される。これを計算すると、

【数５】

$$Pt(0)-Pt(1)$$
$$=\int_{T\min}^{T\min+\frac{\Delta T}{N}}\left\{F(t)-F\left(t+\frac{\Delta T}{N}\right)+F\left(t+\frac{2\Delta T}{N}\right)-F\left(t+\frac{3\Delta T}{N}\right)+\cdots-F\left(t+\frac{(N-2)\Delta T}{N}\right)+F\left(t+\frac{(N-1)\Delta T}{N}\right)\right\}dt \quad \cdots(5)$$

が求められる。

【００２７】

また、分割数Ｎが偶数となる場合の０と１が出る頻度の差はＰｔ（０）－Ｐｔ（１）で表され、これを計算すると

【数６】

$$Pt(0)-Pt(1)$$
$$=\int_{T\min}^{T\min+\frac{\Delta T}{N}}\left\{F(t)-F\left(t+\frac{\Delta T}{N}\right)+F\left(t+\frac{2\Delta T}{N}\right)-F\left(t+\frac{3\Delta T}{N}\right)+\cdots+F\left(t+\frac{(N-3)\Delta T}{N}\right)-F\left(t+\frac{(N-2)\Delta T}{N}\right)\right\}dt$$
$$+\int_{T\min}^{T\min+\frac{\Delta T}{N}}F\left(t+\frac{(N-1)\Delta T}{N}\right) \quad \cdots(6)$$

が求められる。

【００２８】

式（５）及び式（６）より分割数Ｎが偶数、奇数に関わらず、分割数Ｎの値が大きい程「０」と「１」の出現する頻度の差は小さくなる。すなわち、クロック信号ＣＳの周波数が高いほど、「０」と「１」の出現する頻度に偏りがなくなることを示している。つまり、乱数を生成する場合は、使用する乱数の特性を考慮しクロック信号の周波数を選定する必要がある。

【００２９】

さらに、理想値０．５と０が出現する確率との差δ（０）は、

【数７】

$$\delta(0) = 0.5 - |(Pt(0) / (Pt(0) + Pt(1))|$$

・・・・・（７）

で表される。

【００３０】

また、理想値０．５と１が出現する確率との差δ（１）は、

【数８】

$$\delta(1) = 0.5 - |(Pt(0) / (Pt(0) + Pt(1))|$$

・・・・・（８）

で表される。

【００３１】

δ（０）とδ（１）は、米国商務省が定めるＦＩＰＳ１４０［１］という規格検定によって利用分野により基準値が定められている。例えば、乱数生成回路を通信ネットワークのセキュリティに用いる場合は、δ（０）またはδ（１）の値が０．０１３７５以下でなければならない。すなわち、クロック信号ＣＫの周波数を基準値を満たすよう設定する必要がある。

【００３２】

また、ランダム信号ＲＳは、オン幅Ｔ、オフ幅が一定でないので、振幅、周期、及び位相等の有限個のパラメータで特性を表現することができない。そこで、ランダム信号ＲＳを表現する方法としては、信号のパワーを一定の周波数帯域毎に分割し、各帯域毎のパワーを周波数の関数として表したパワースペクトルが用いられる。周期的信号波形のスペクトルは、基本周波数とその高調波成分から成り立っており、各成分の振幅の二乗の和で表すことができる。パワースペクトルは、時間関数ｘ（ｔ）、パワースペクトルＸ（ｆ）とすると、

【数９】

$$X(f) = \int_0^\infty x(t)e^{-j2\pi ft}\,dt \quad \cdots(9)$$

で表される。

【００３３】

乱数生成回路１０ａに入力されるランダム信号ＲＳは、図４に示すように、縦軸で示すパワースペクトルの信号強度が、横軸で示す周波数に対し反比例の関係にあるとする。この時、図５に示すように、ランダム信号ＲＳがオン幅Ｔである頻度の分布は、パワースペクトル特性で示す横軸方向を周波数から周期に変えた横軸方向に対称な曲線で示される。オン幅がＴ（ｓ）である時の乱数生成回路の出力は、クロック信号ＣＳの周期$Ｔ_{ｃｋ}$毎に「０」または「１」を出力するかが決まる。クロック信号ＣＳの周期が小さい程、「０」と「１」が出現する確率はそれぞれ０．５に近くなる。

【００３４】

図６で示すＬ１は、図１で示す乱数生成回路１０ａから出力される乱数信号ＲＮＳのパワースペクトルを表す。また、Ｌ２は、１／ｆノイズ源から生成されるランダム信号ＲＳのパワースペクトルを表す。ランダム信号ＲＳに対するパワースペクトルが周波数が高くなると減少してしまうのに対し、乱数信号ＲＮＳのパワースペクトルＬ１は周波数特性に依存せず乱数信号ＲＮＳを生成することができる。

【００３５】

更に、ランダム信号ＲＳを８ビットのシリアルデータとして入力した場合、前回のデータを縦軸で示す０～２５５に、次に取得されるデータを横軸に続けて２５００点プロットする。この時、乱数生成回路１０ａから出力される乱数信号ＲＮＳは、図７（ａ）に示すように、ほぼ均一に分布する。これに対し、従来の乱数生成回路から出力される乱数は、図７（ｂ）に示すように、バラツキが生じる。

【００３６】

本発明の第１の実施の形態に係る乱数生成回路１０ａによれば、複数の雑音発生回路を用いず、小型化が可能であり、周波数特性に依存しない乱数を生成し、「０」と「１」の出現する確率の調整を不要とすることが可能となる。

【００３７】

（第２の実施の形態）

本発明の第２の実施の形態に係る乱数生成回路１０ｂは、図８に示すように、図１に示す乱数生成回路１０ａの第１のラッチ回路３の出力側に第２のラッチ回路４を１段追加している点で異なる。第２のラッチ回路４の入力端子Ｄは、第１のラッチ回路３の出力端子Ｑに電気的に接続される。また、第２のラッチ回路４の出力端子Ｑは、乱数出力端子５３に接続される。クロック入力端子ＣＫは乱数取得クロック入力端子５４にそれぞれ接続されている。乱数取得クロック入力端子５４は、周期が一定である乱数クロック取得信号を入力する端子である。他は第１の実施の形態と実質的に同様であるので、重複した記載を省略する。

【００３８】

次に、本発明の第２の実施の形態に係る乱数生成回路の動作を図９を用いて説明する。

【００３９】

（イ）先ず、時刻ｔ１において、図９（ａ）に示すように、矩形波入力端子５１に入力されるランダム信号ＲＳがローレベルからハイレベルとなる。

【００４０】

（ロ）時刻ｔ１からｔ２までの間、ランダム信号ＲＳがハイレベルの状態では、クロック信号ＣＳの立ち上がりエッジ検出毎に、カウンタ回路１の出力端子Ｑから出力されるカウント信号ＣＴＳのレベルは交互に切り替わる。

【００４１】

（ハ）時刻ｔ２において、ランダム信号ＲＳがハイレベルからローレベルとなる。ランダム信号ＲＳがローレベルとなると、インバータ２は、図９（ｄ）に示すように、ハイレベルとなるランダム反転信号ＲＳバーを出力する。ランダム反転信号ＲＳバーがハイレベルとなると、第１のラッチ回路３は、クロック入力端子ＣＫの立ち上がりエッジでカウンタ回路１から出力されるカウント信号ＣＴＳをラッチし、図９（ｅ）に示すように、第１の乱数信号ＲＮＳ１を出力する。

【００４２】

（ニ）時刻ｔ３において、図９（ｆ）に示すように、周期が一定である乱数取得クロック信号ＲＴＳがローレベルからハイレベルとなる。第２のラッチ回路４は、乱数取得クロック信号ＲＴＳの立ち上りエッジで第１の乱数信号ＲＮＳ１を

ラッチし、図９（ｇ）に示すように、第２の乱数信号ＲＮＳ２を出力する。以後、同様にランダム信号ＲＳの立ち下がりエッジで乱数信号ＲＮＳを出力する動作を繰り返す。

【００４３】

本発明の第２の実施の形態に係る乱数生成回路１０ｂによれば、複数の雑音発生回路を用いず、小型化が可能であり、周波数特性に依存しない乱数を生成し、「０」と「１」の出現する確率の調整を不要とすることが可能となる。また、第２のラッチ回路４から出力される乱数信号ＲＮＳを用いることにより一定時間間隔で乱数を取得することができる。

【００４４】

（第３の実施の形態）

本発明の第３の実施の形態に係る乱数生成回路１０ｃは、図１０に示すように、図１に示す乱数生成回路１０ａのカウンタ回路１のカウントイネーブル端子ＣＥと矩形波入力端子５１との間にパルスカウンタ５を備える点が異なる。パルスカウンタ５は、入力側を矩形波入力端子５１に、出力側をカウンタ回路１のカウントイネーブル端子ＣＥにそれぞれ電気的に接続する。他は第１の実施の形態と実質的に同様であるので、重複した記載を省略する。

【００４５】

本発明の第３の実施の形態に係る乱数生成回路１０ｃの動作を、図１１を用いて説明する。

【００４６】

（イ）先ず、時刻ｔ１において、図１１（ａ）に示す第１のランダム信号ＲＳ１がローレベルからハイレベルとなる。パルスカウンタ５は、第１のランダム信号ＲＳ１の立ち上がりエッジを検出すると、図１１（ｂ）に示すように、ハイレベルとなる第２のランダム信号ＲＳ２を出力する。

【００４７】

（ロ）時刻ｔ１からｔ２までの間、ランダム信号ＲＳがハイレベルの状態となる。この時、図１１（ｄ）に示すように、カウンタ回路１の出力端子Ｑから出力されるカウント信号ＣＴＳのレベルは、図１１（ｃ）に示すクロック信号ＣＳの

立ち上がりエッジ検出毎に交互に切り替わる。また、パルスカウンタ５は、ランダム信号ＲＳ１の立ち上がりエッジをカウントする。ただし、パルスカウンタ５は例示的にカウント値が２になると出力を切り替えるとする。

【００４８】

（ハ）時刻ｔ２において、パルスカウンタ５のカウント値が２になると、第２のランダム信号ＲＳ２はハイレベルからローレベルとなる。第２のランダム信号ＲＳ２がローレベルとなると、図１１（ｄ）に示すように、第１のラッチ回路３のクロック入力端子ＣＫはハイレベルとなる。第１のラッチ回路３は、クロック入力端子ＣＫの立ち上がりエッジでカウンタ回路１から出力されるカウント信号ＣＴＳをラッチし、乱数出力端子５３に乱数信号ＲＮＳを出力する。以後、同様にランダム信号ＲＳの立ち下がりエッジで乱数信号ＲＮＳを出力する動作を繰り返す。

【００４９】

本発明の第３の実施の形態に係る乱数生成回路１０ｃによれば、複数の雑音発生回路を用いず、小型化が可能であり、周波数特性に依存しない乱数を生成し、「０」と「１」の出現する確率の調整を不要とすることが可能となる。また、ランダム信号の最小オン幅T_{min}がクロック信号ＣＳの周期T_{ck}に対し２倍以下であっても動作させることが可能となる。

【００５０】

（第４の実施の形態）

本発明の第４の実施の形態に係る乱数生成回路１０ｄは、図１２に示すように、オン幅及びオフ幅が一定でないランダム信号ＲＳとクロック信号ＣＳを入力し、ランダム信号ＲＳ及びクロック信号ＣＳの論理積出力の変化に応じてハイレベルとローレベルを交互に切り替える分周信号ＤＲＳを出力する分周回路６と、ランダム信号ＲＳの変化に応じて分周信号ＤＲＳをラッチし乱数信号ＲＮＳを出力する第１のラッチ回路３とを備える。

【００５１】

分周回路６は、第１の入力端子を矩形波入力端子５１に、第２の入力端子をクロック入力端子５２にそれぞれ接続されるアンド回路２０と、アンド回路２０の

出力端子をクロック入力端子に接続する分周ラッチ回路２１と、分周ラッチ回路２１の出力端子Ｑと入力端子Ｄとの間に接続されたインバータ２２とを備える。

【００５２】

本発明の第４の実施の形態に係る乱数生成回路１０ｄの動作を図１３を用いて説明する。

【００５３】

（イ）先ず、図１３（ａ）に示すように、時刻ｔ１において、矩形波入力端子５１に入力されるランダム信号ＲＳがローレベルからハイレベルとなる。

【００５４】

（ロ）時刻ｔ１からｔ２までの間、ランダム信号ＲＳがハイレベルの状態では、図１３（ｃ）に示すように、アンド回路２０の出力端子から図１３（ｂ）に示すクロック信号ＣＳがそのまま出力される。この時、図１３（ｄ）に示すように、クロック信号ＣＳの立ち上がりエッジ検出毎に分周ラッチ回路２１の出力端子Ｑから出力される分周信号ＤＲＳのレベルは交互に切り替わる。

【００５５】

（ハ）時刻ｔ２において、ランダム信号ＲＳがハイレベルからローレベルとなると、図１３（ｅ）に示すように、第１のラッチ回路３のクロック入力端子ＣＫはハイレベルとなる。クロック入力端子ＣＫがハイレベルとなると、第１のラッチ回路３は分周信号ＤＲＳをラッチし、図１３（ｆ）に示すように、乱数出力端子５３から乱数信号ＲＮＳを出力する。以後、同様にランダム信号ＲＳの立ち下がりエッジで乱数信号ＲＮＳを出力する動作を繰り返す。

【００５６】

本発明の第４の実施の形態に係る乱数生成回路１０ｄによれば、複数の雑音発生回路を用いず、小型化が可能であり、周波数特性に依存しない乱数を生成し、「０」と「１」の出現する確率の調整を不要とすることが可能となる。

【００５７】

（第５の実施の形態）

本発明の第５の実施の形態に係る乱数生成回路１０ｅは、図１４に示すように、図１２で示す乱数生成回路１０ｄが分周ラッチ回路としてラッチ回路２１（Ｄ

型フリップフロップ）を用いているのに対し、ラッチ回路２３（Ｊ－Ｋ型フリップフロップを用いる点で異なる。また、第１のラッチ回路３（Ｄ型フリップフロップ）もを用いているのに対し、ラッチ回路７（Ｊ－Ｋ型フリップフロップ）を用いる点で異なる。他は第１の実施の形態と実質的に同様であるので、重複した記載を省略する。

【００５８】

本発明の第５の実施の形態に係る乱数生成回路１０ｅの動作を、図１５を用いて説明する。

【００５９】

（イ）先ず、時刻ｔ１において、図１５（ａ）に示すように、ランダム信号ＲＳがローレベルからハイレベルとなる。

【００６０】

（ロ）時刻ｔ１からｔ２までの間、ランダム信号ＲＳがハイレベルの状態では、図１５（ｃ）に示すように、アンド回路２０の出力端子から図１５（ｂ）に示すクロック信号ＣＳがそのまま出力される。この時、図１５（ｄ）に示すように、クロック信号ＣＳの立ち上がりエッジ検出毎に分周ラッチ回路２３の出力端子Ｑから出力される分周信号ＤＲＳのレベルは交互に切り替わる。

【００６１】

（ハ）時刻ｔ２において、ランダム信号ＲＳがハイレベルからローレベルとなると、図１５（ｆ）に示すように、ラッチ回路７のクロック入力端子ＣＫはハイレベルとなる。この時、ラッチ回路７の第１の入力端子Ｊには、図１５（ｄ）に示すように、分周信号ＤＲＳが入力される。また、ラッチ回路７の第２の入力端子Ｋには、図１５（ｅ）に示すように、分周信号ＤＲＳを反転した分周反転信号ＤＲＳバーが入力される。ラッチ回路７は、ランダム信号ＲＳを反転したランダム反転信号ＲＳバーの立ち上がりエッジで分周信号ＤＲＳをラッチし、図１５（ｇ）に示すように、乱数信号ＲＮＳを出力する。乱数信号ＲＮＳは乱数信号出力端子５３から出力される。以後、同様にランダム信号ＲＳの立ち下がりエッジで乱数信号ＲＮＳを出力する動作を繰り返す。

【００６２】

本発明の第５の実施の形態に係る乱数生成回路１０ｅによれば、複数の雑音発生回路を用いず、小型化が可能であり、周波数特性に依存しない乱数を生成し、「０」と「１」の出現する確率の調整を不要とすることが可能となる。

【００６３】

（その他の実施の形態）

上記のように、本発明は第１～第５の実施の形態によって記載したが、この開示の一部をなす論述及び図面はこの発明を限定するものであると理解すべきではない。この開示から当業者には様々な代替実施の形態、実施例及び運用技術が明らかとなろう。

【００６４】

既に述べた第４～第５の実施の形態に係る乱数生成回路１０ｄ、１０ｅについては、第２の実施の形態で示すような第２のラッチ回路を更に設けることが可能である。また、乱数生成回路１０ｄ、１０ｅは、第３の実施の形態で示すように、ラッチ回路の出力に、更にパルスカウンタを設けることも可能である。

【００６５】

既に述べた第１～第５の実施の形態に係る乱数生成回路１０ａ、１０ｂ、１０ｃ、１０ｄ、１０ｅで用いられるクロック信号ＣＳの周期は、ランダム信号ＲＳの最小オン幅T_{min}の２倍以上であることが望ましい。クロック信号ＣＳの周期Ｔを最小オン幅T_{min}に対して大きく設定するほどランダム信号ＲＳのパワースペクトルの差異による影響を抑えることができる。

【００６６】

このように、本発明はここでは記載していない様々な実施の形態等を含むことは勿論である。したがって、本発明の技術的範囲は上記の説明から妥当な特許請求の範囲に係る発明特定事項によってのみ定められるものである。

【００６７】

【発明の効果】

本発明によれば、複数の雑音発生回路を用いず、小型化が可能であり、周波数特性に依存しない乱数を生成し、「０」と「１」の出現する確率の調整を不要とすることが可能な乱数生成回路を提供することができる。

【図面の簡単な説明】

【図１】

本発明の第１の実施の形態に係る乱数生成回路を説明する図である。

【図２】

本発明の第１の実施の形態に係る乱数生成回路の動作タイミングチャートである。

【図３】

本発明の第１の実施の形態に係る乱数生成回路に入力するランダム信号を説明する図である。

【図４】

本発明の第１の実施の形態に係るランダム信号のパワースペクトルを模式的に説明する図である。

【図５】

本発明の第１の実施の形態に係る乱数生成回路により生成される乱数信号を説明する図である。

【図６】

本発明の第１の実施の形態に係る乱数生成回路により生成される乱数信号のパワースペクトルを説明する図である。

【図７】

図７（ａ）は、本発明の第１の実施の形態に係る乱数生成回路により生成される乱数信号の周期性を説明する図である。

図７（ｂ）は、従来の乱数生成回路により生成される乱数信号の周期性を説明する図である。

【図８】

本発明の第２の実施の形態に係る乱数生成回路を説明する図である。

【図９】

本発明の第２の実施の形態に係る乱数生成回路の動作タイミングチャートである。

【図１０】

本発明の第３の実施の形態に係る乱数生成回路を説明する図である。

【図１１】

本発明の第３の実施の形態に係る乱数生成回路の動作タイミングチャートである。

【図１２】

本発明の第４の実施の形態に係る乱数生成回路を説明する図である。

【図１３】

本発明の第４の実施の形態に係る乱数生成回路の動作タイミングチャートである。

【図１４】

本発明の第５の実施の形態に係る乱数生成回路を説明する図である。

【図１５】

本発明の第５の実施の形態に係る乱数生成回路の動作タイミングチャートである。

【図１６】

従来の乱数生成回路について説明する図である。

【符号の説明】

１…カウンタ回路

２，２２…インバータ

３…第１のラッチ回路

４…第２のラッチ回路

５…パルスカウンタ

６…分周回路

１０ａ，１０ｂ，１０ｃ，１０ｄ，１０ｅ…乱数生成回路

２０…アンド回路

２１…分周ラッチ回路

５１…矩形波入力端子

５２…クロック入力端子

５３…乱数出力端子

５４…乱数取得クロック入力端子

２０１，２０２…雑音発生回路

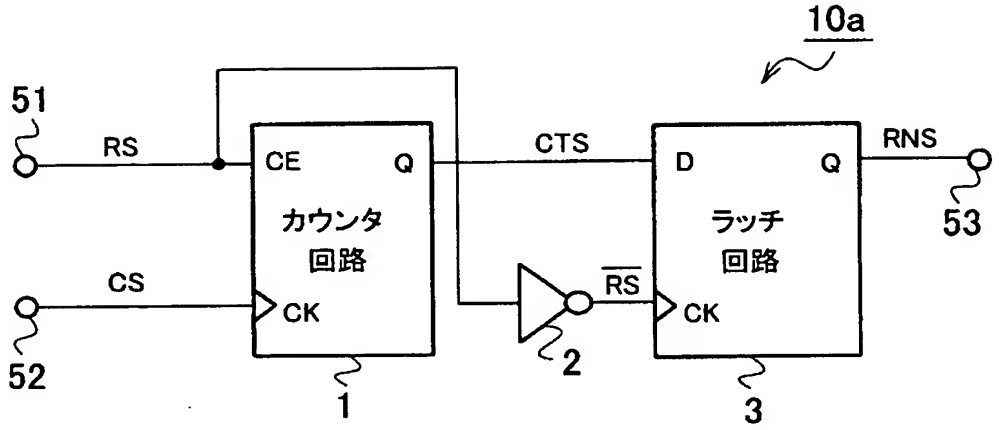
２０３…差動回路

２０４…Ｄ変換回路

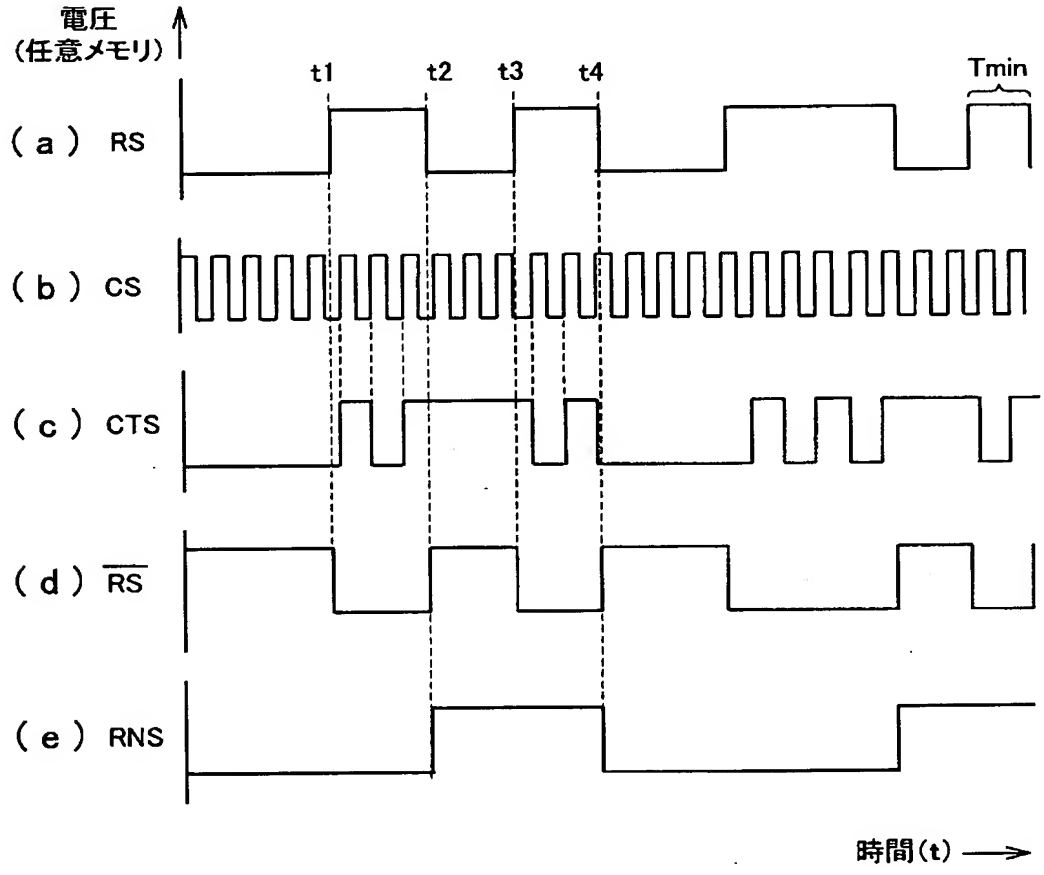
２０５…演算回路

【書類名】　　図面

【図１】

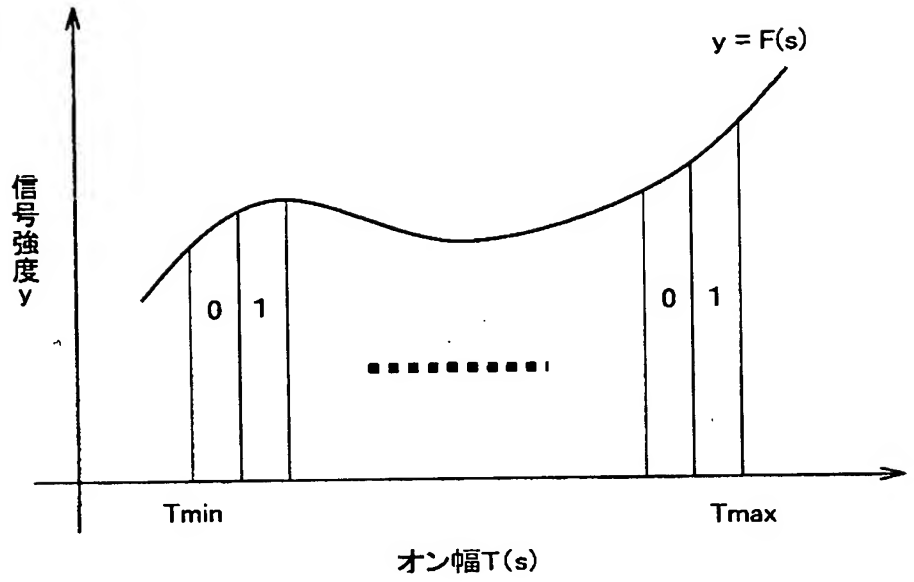


【図２】

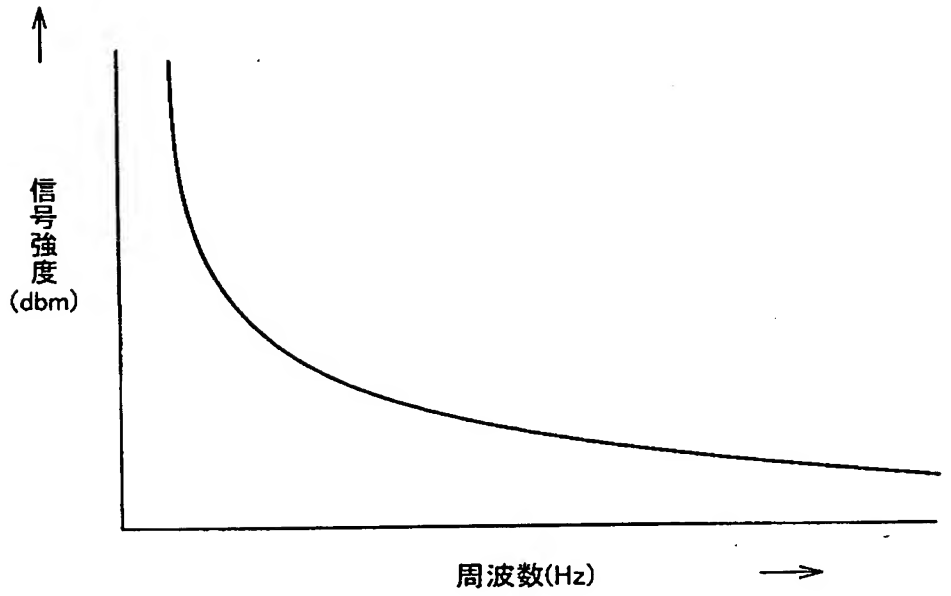


出証特２００３－３０２３４６４

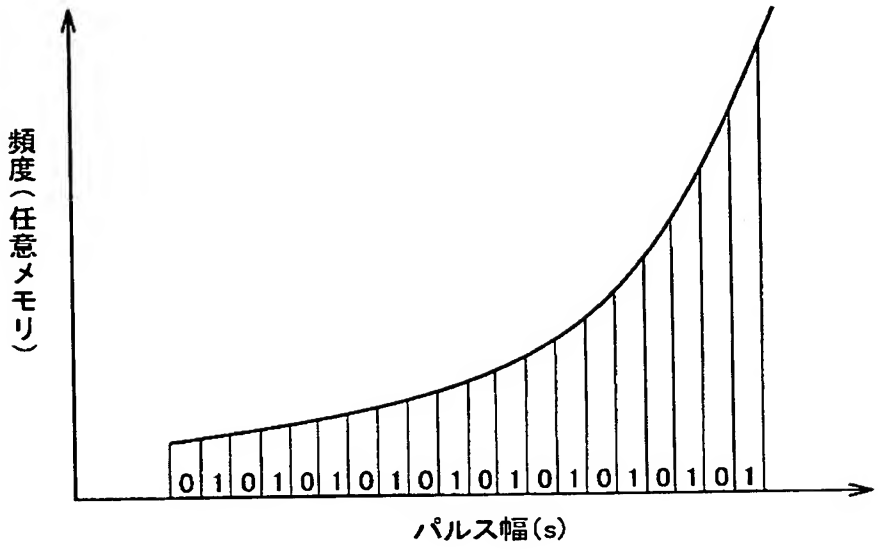
【図３】



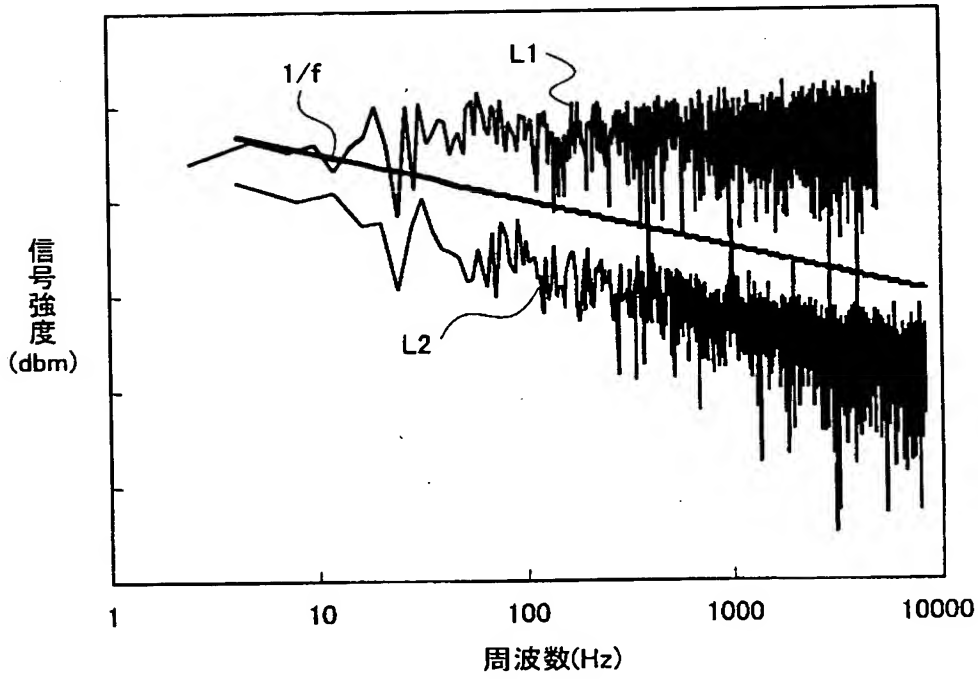
【図４】



【図５】

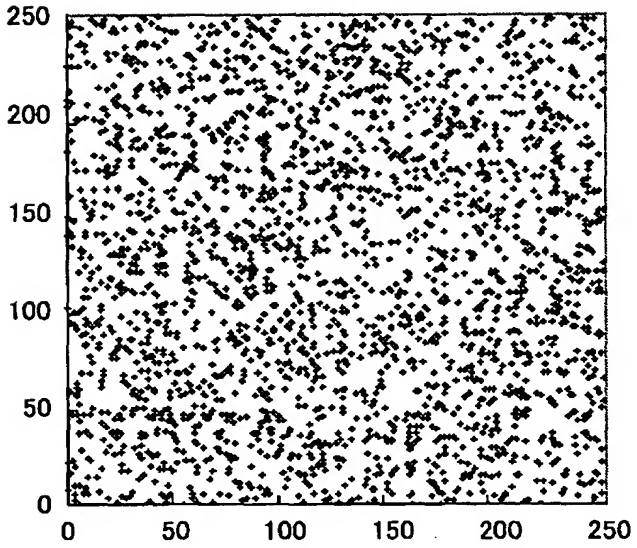

頻度（任意メモリ）
0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1
パルス幅(s)

【図６】

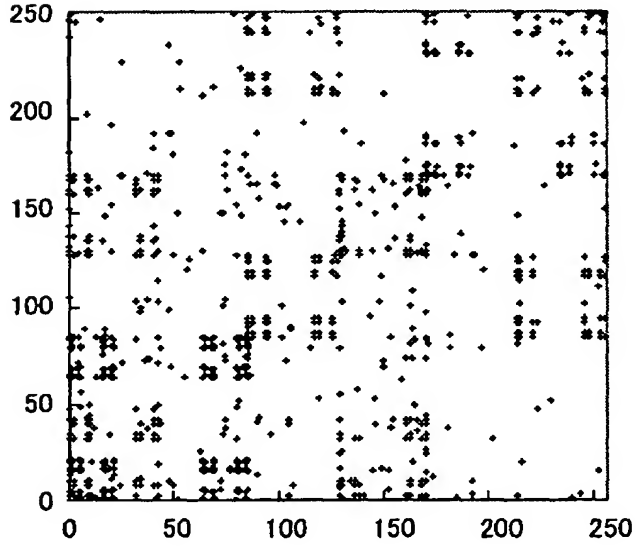

1/f
L1
L2
信号強度(dbm)
1
10
100
1000
10000
周波数(Hz)

【図７】

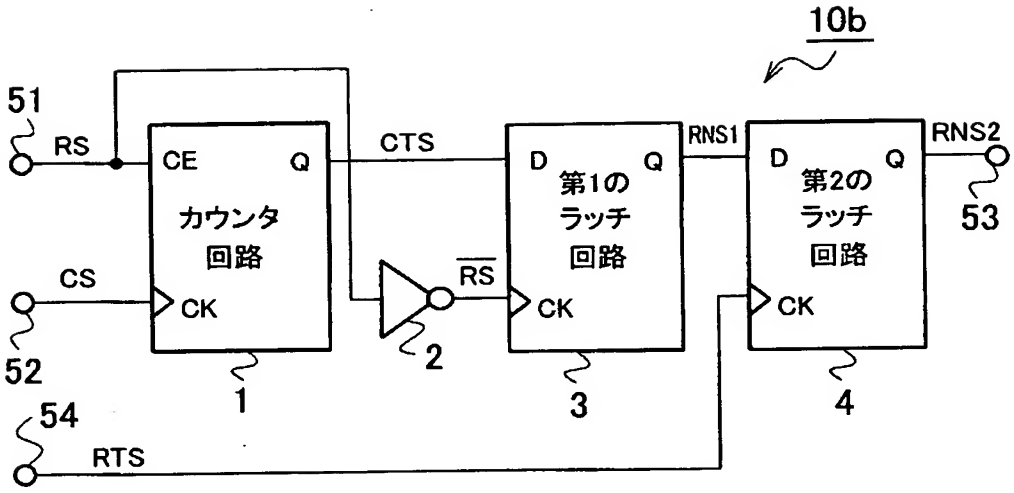
（ａ）


250
200
150
100
50
0
0
50
100
150
200
250

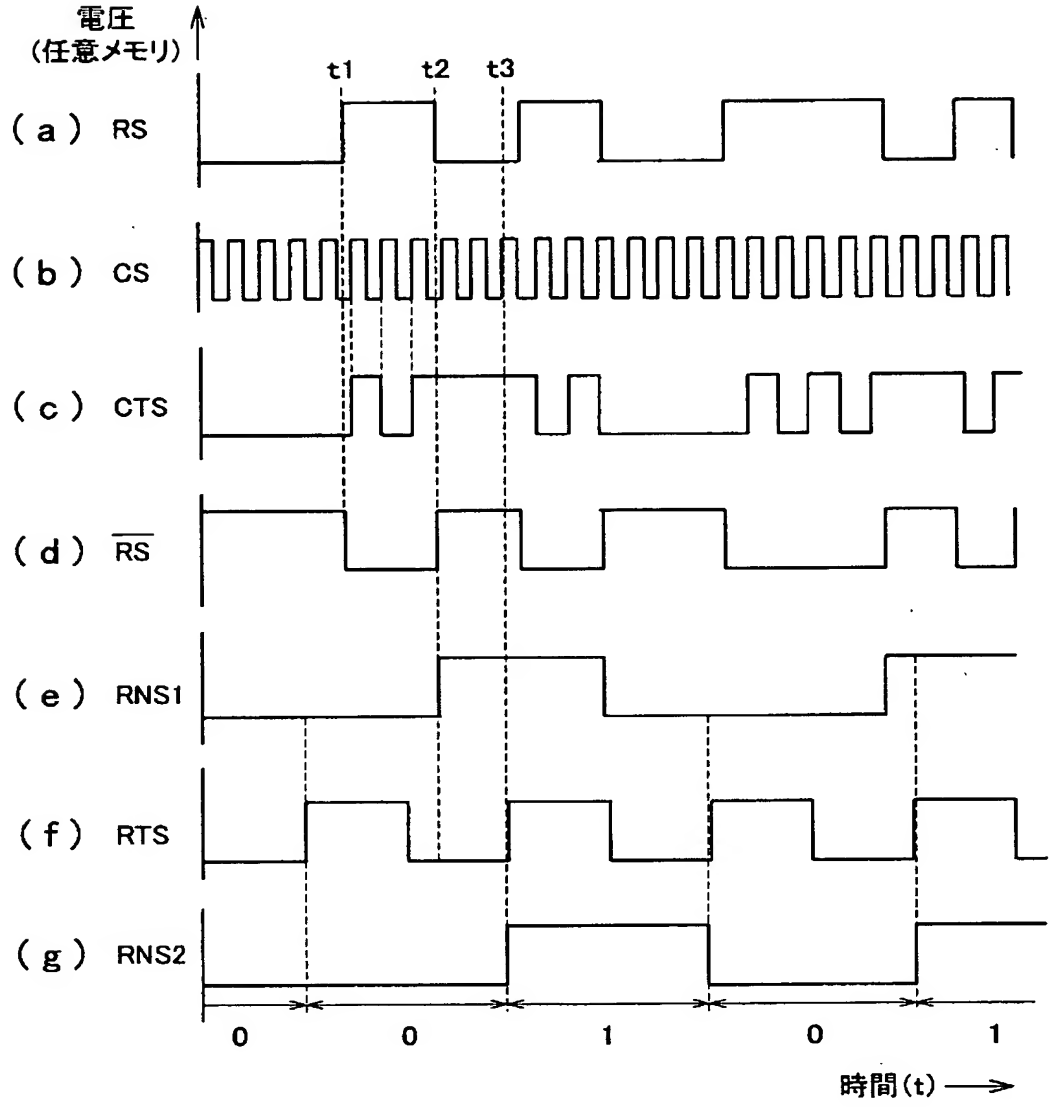
（ｂ）


250
200
150
100
50
0
0
50
100
150
200
250

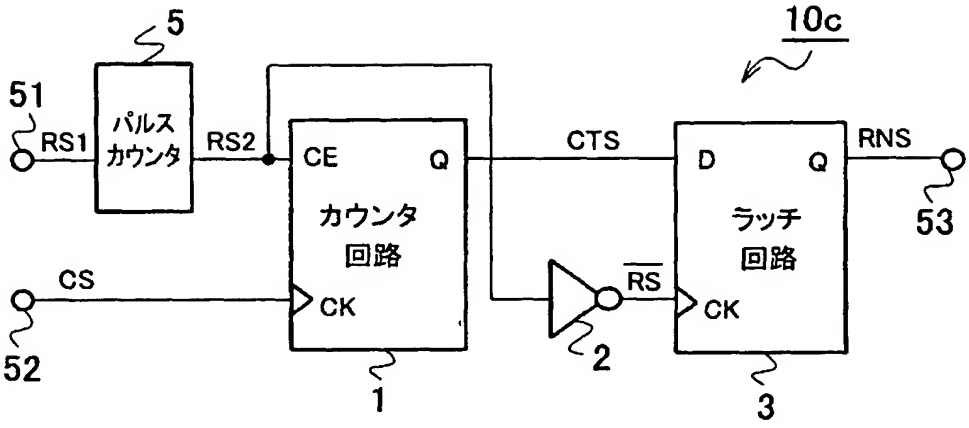
【図８】


10b
51
RS
CE
Q
CTS
D
Q
RNS1
D
Q
RNS2
カウンタ
回路
第1の
ラッチ
回路
第2の
ラッチ
回路
53
CS
CK
RS
CK
CK
52
1
2
3
4
54
RTS

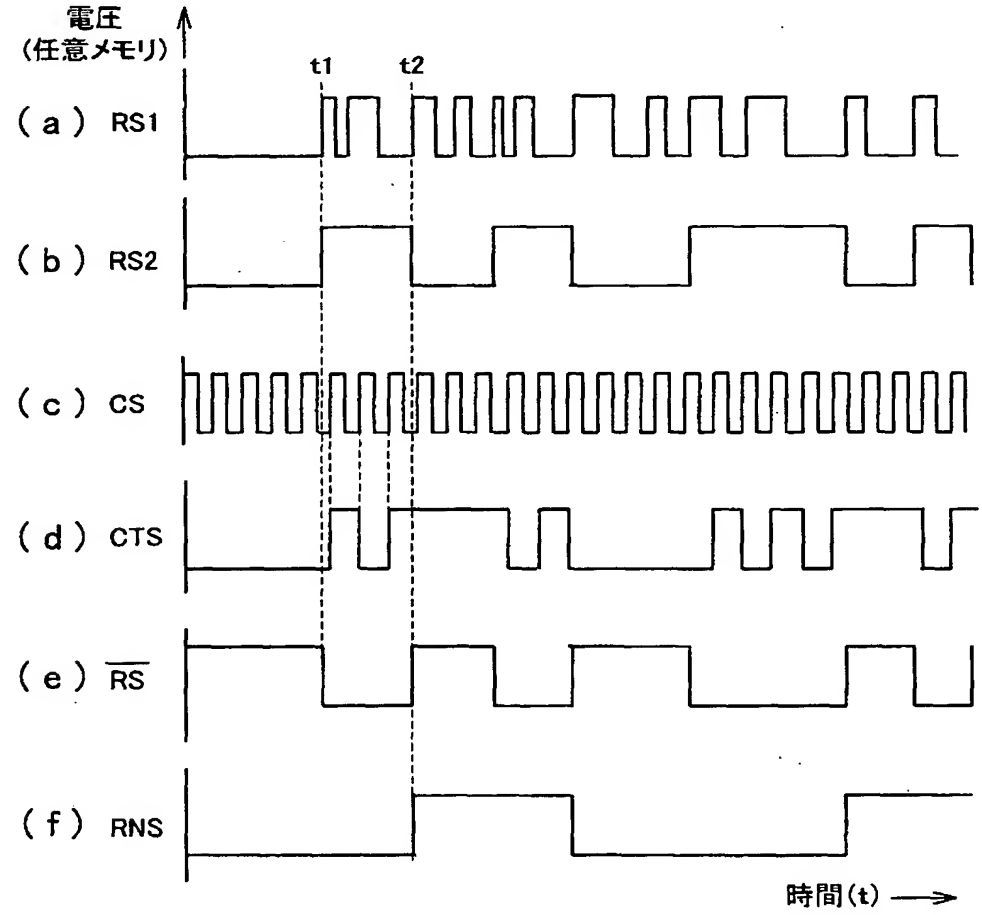
【図９】


電圧
(任意メモリ)
t1
t2
t3
(a) RS
(b) CS
(c) CTS
(d) $\overline{RS}$
(e) RNS1
(f) RTS
(g) RNS2
0
0
1
0
1
時間(t)

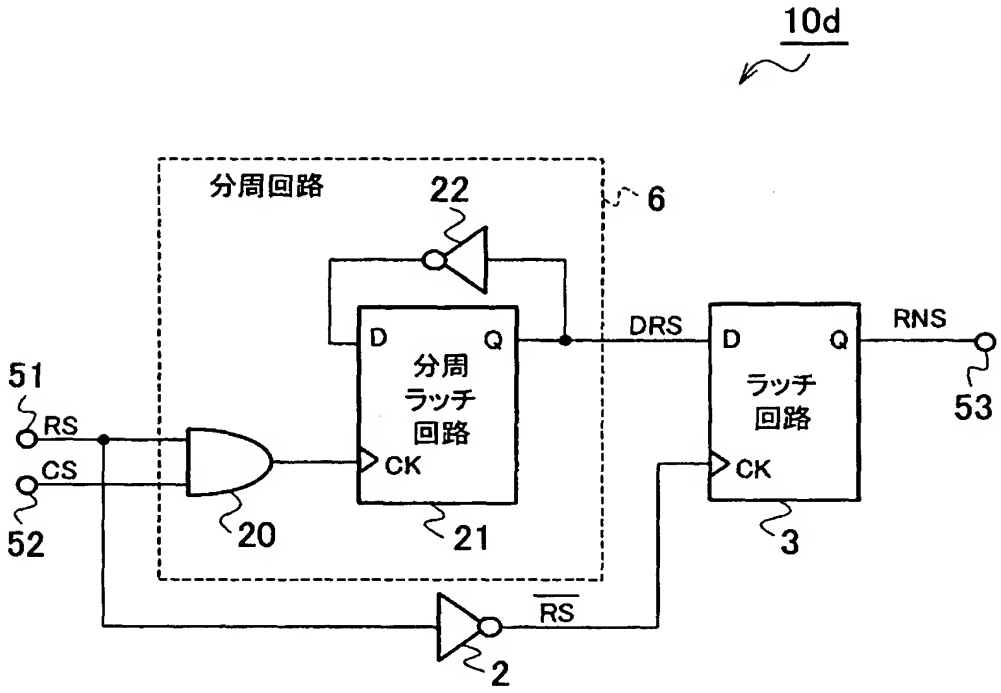
【図１０】


5
10c
51
RS1
パルス
カウンタ
RS2
CE
Q
CTS
D
Q
RNS
53
カウンタ
回路
ラッチ
回路
CS
CK
RS
CK
52
2
1
3

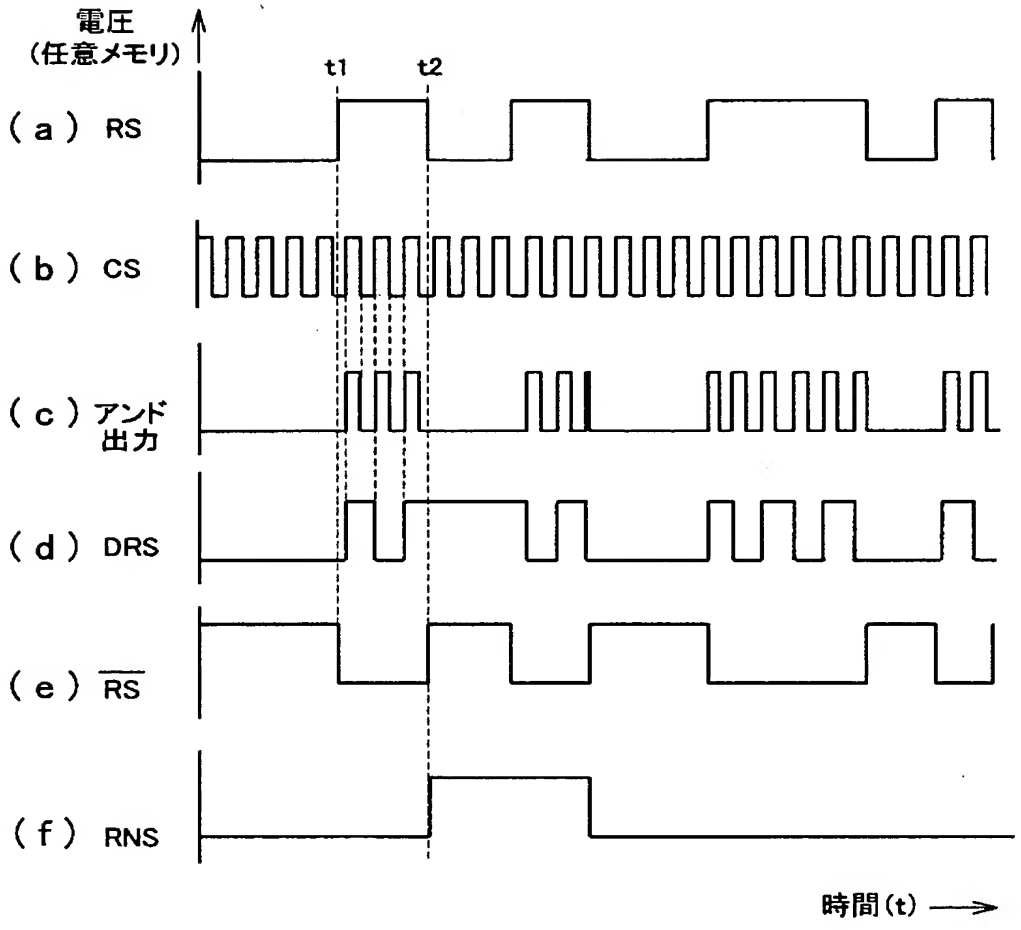
【図１１】


電圧
(任意メモリ)
t1
t2
(a) RS1
(b) RS2
(c) CS
(d) CTS
(e) RS
(f) RNS
時間(t)

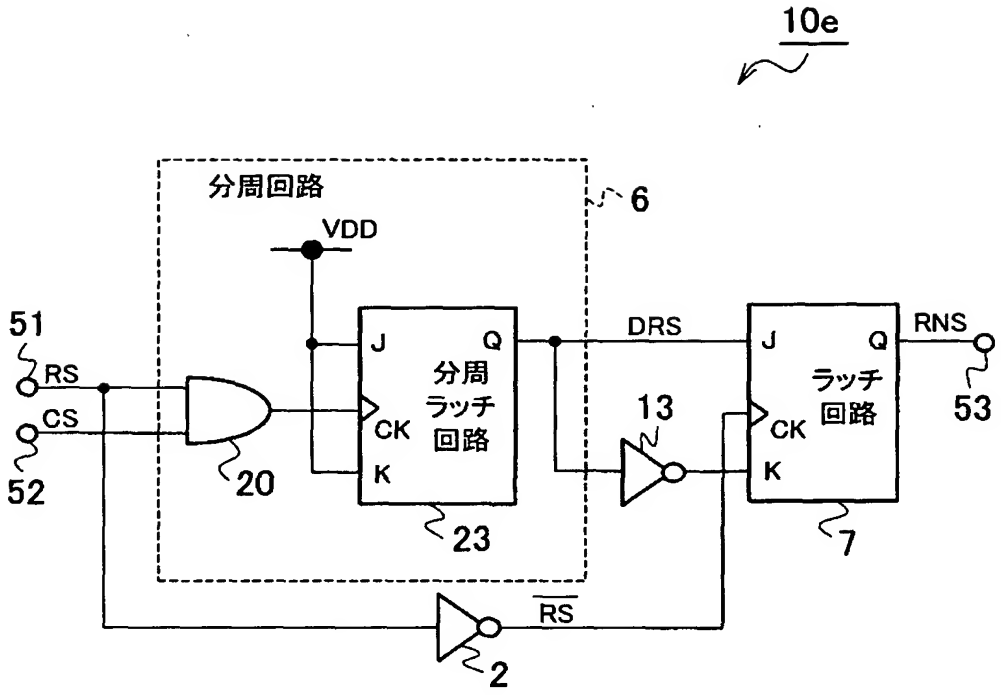
【図１２】


10d
分周回路
22
6
D
Q
分周
ラッチ
回路
CK
21
DRS
D
Q
ラッチ
回路
CK
3
RNS
53
51
RS
CS
52
20
RS
2

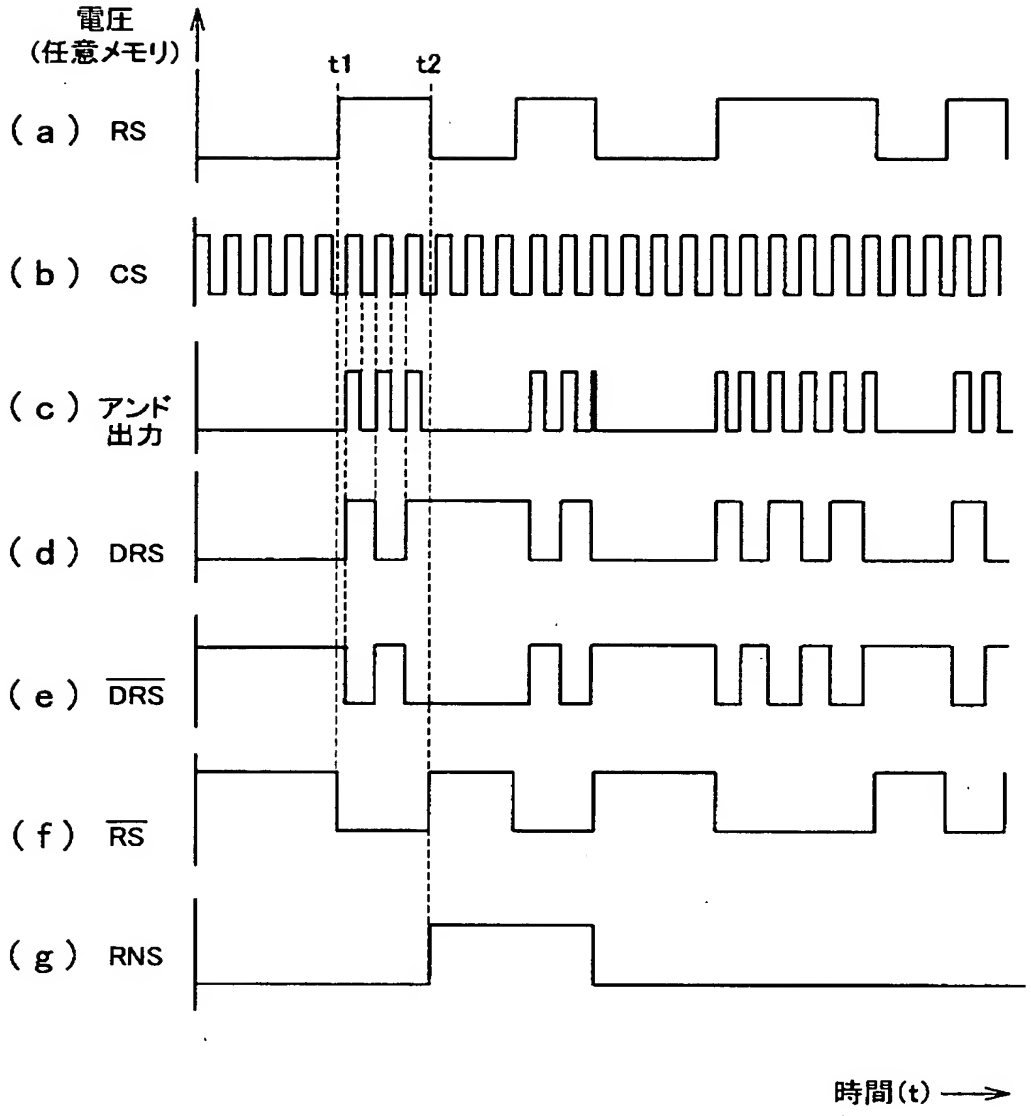
【図１３】



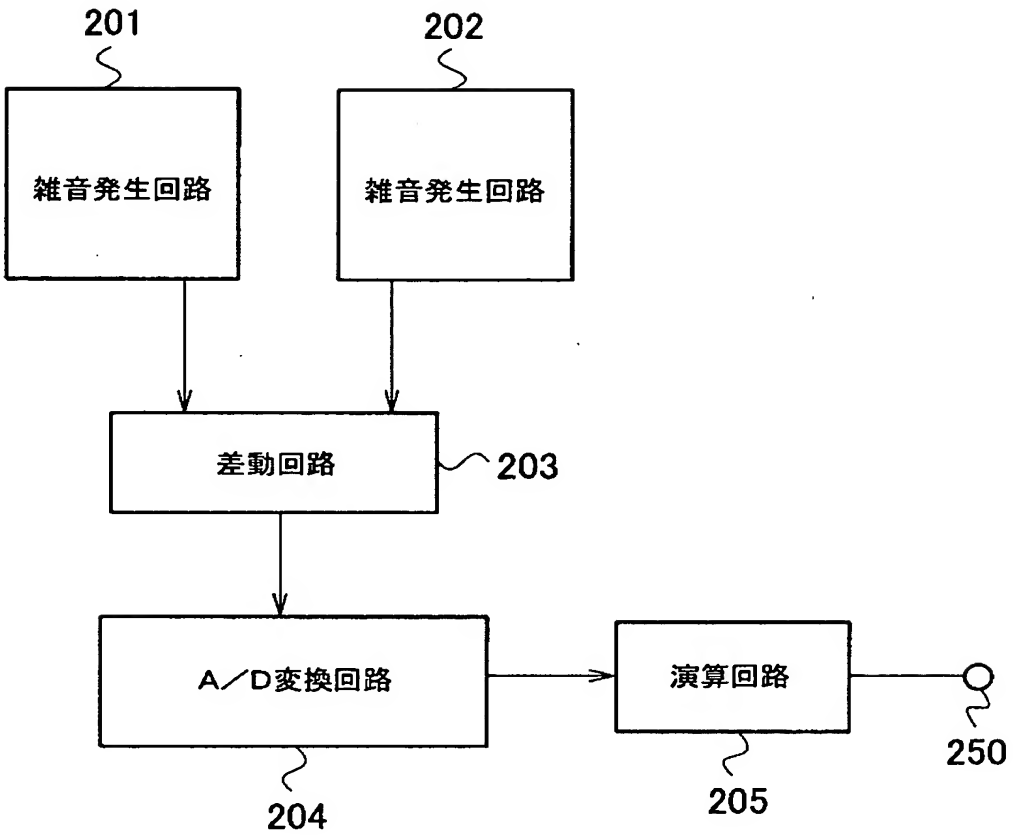
【図１４】


10e
分周回路
6
VDD
51
RS
CS
52
20
J
Q
CK
K
分周
ラッチ
回路
23
DRS
13
J
Q
CK
K
ラッチ
回路
7
RNS
53
RS
2

【図１５】


電圧
(任意メモリ)
t1
t2
(a) RS
(b) CS
(c) アンド出力
(d) DRS
(e) $\overline{DRS}$
(f) $\overline{RS}$
(g) RNS
時間(t)

【図１６】



【書類名】　　要約書

【要約】

【課題】　複数の雑音発生回路を用いず、小型化が可能であり、周波数特性に依存しない乱数を生成し、「０」と「１」の出現する確率の調整を不要とすることが可能な乱数生成回路を得る。

【解決手段】　ランダム信号ＲＳとクロック信号ＣＳを入力し、ランダム信号ＲＳの変化に応じてクロック信号ＣＳのカウント値を出力するカウンタ回路１と、ランダム信号ＲＳの変化に応じてカウント値をラッチし乱数信号ＲＮＳを出力する第１のラッチ回路３とを備える。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００３０７８〕

１．変更年月日　　２００１年　７月　２日
［変更理由］　住所変更
住　所　　東京都港区芝浦一丁目１番１号
氏　名　　株式会社東芝